IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF: THE RESIDENCE LOCATED AT 1008 21ST AVE., ALTOONA, PA 16601	Magistrate No. 3:21-154 MJ **[UNDER SEAL]**

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Jason Adams, a Special Agent (SA) with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Pittsburgh, Pennsylvania, Office. I have been so employed since July 2009. As part of my duties as an HSI Special Agent, I investigate criminal violations relating to high technology crime, cyber-crime, child exploitation and child pornography including violations pertaining to the illegal distribution, receipt, possession, and production of materials depicting the sexual exploitation of children. I have received training in the area of child exploitation offenses and I have conducted and assisted in several child exploitation investigations. I have executed numerous search warrants related to child exploitation investigations. In this regard, I have reviewed extensive samples of child pornography, including videos, photographs, and digital reproductions of photographs or other print media. I am also responsible for enforcing federal criminal statutes involving immigration and customs violations.

2. This affidavit is made in support of an application for a search warrant for the entire premises located at **1008 21ST AVE., ALTOONA, PA 16601**, for items specified in "Attachment B." The residence is specifically described in "Attachment A."

3. The purpose of this application is to seize evidence, fruits, and instrumentalities, more particularly described in Attachment B, of violations of Title 18, United States Code, Section 2252(a)(2), which makes it a crime to receive and distribute material depicting the sexual exploitation of a minor; and violations of Title 18, United States Code, Section 2252(a)(4)(B), which makes it a crime to possess material depicting the sexual exploitation of a minor and access with intent to view it.

4. Through my experience and training, I am aware that Title 18, United States Code, Section 2256 defines "minor", for purposes of Section 2252, as "any person under the age of eighteen years". Section 2256 also defines "sexually explicit conduct" for purposes of these sections as including: (a) genital-genital, oral-genital, anal-genital, and oral-anal sexual intercourse, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic; or (e) lascivious exhibition of the genitals or pubic area of any person.

5. The statements in this affidavit are based, in part, on information provided by witnesses and your affiant's investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B) are presently located at **1008 21ST AVE., ALTOONA, PA 16601**.

6. In summary, the following affidavit sets forth facts that establish that there is probable cause to believe that a subject who received, distributed, and/or possessed visual depictions of minors engaged in sexually explicit conduct, via the Internet, is using electronic

devices located at **1008 21ST AVE., ALTOONA, PA 16601** to access said materials. Said visual depictions may be viewed, accessed, saved, and stored on various tangible devices, to include computers, cellular devices, USB "thumb" drives, memory cards, etc., as well as may be printed into hard copy form.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

b. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

c. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

d. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television,

dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

e. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

f. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and

system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

g. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

h. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

i. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

j. The terms "records", "documents", and "materials", as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides,

negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND REGARDING SEIZURE OF COMPUTERS

8. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most of the computer items (hardware, software and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is almost always true because of the following:

9. Computer storage devices (like hard drives, diskettes, laser disks, and others) store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This examination process can take weeks or months, depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

10. Searching computer systems for criminal evidence is a highly technical process requiring expert skills in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some

systems and applications. It is difficult to know before a search which expert should analyze the system and its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

11. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit ("CPU"). In cases like this one, where the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

BACKGROUND REGARDING THE INTERNET

12. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I have conducted numerous searches and forensic reviews of computers, cellular communications devices and other digital storage media. I have formal training on conducting computer-based investigations.

13. Through my training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know that the Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing; that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

14. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

15. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

16. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading". The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer).

17. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

OVERVIEW OF PEER-TO-PEER FILE SHARING

18. A significant aspect of the Internet is peer to peer (P2P) file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. These P2P networks are commonly referred to as decentralized networks because each user of the network is able to distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent, where all of the information is first deposited before it is distributed. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. However, only files that are specifically stored in shared folders are exchanged. Therefore, a user needs simply to move a file from the shared folder to another folder to stop the distribution across the Internet.

19. BitTorrent is one type of P2P file sharing software. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "infohash", which uniquely identifies the torrent based on the file(s) associated with the torrent file. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts or the actual file(s) being sought. The download of

the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

20. One of the advantages of P2P file sharing is that multiple files may be downloaded at the same time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading a file may actually receive parts of the file from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. However, a BitTorrent user downloading a file may receive the entire file from just one computer. A user may also add other files into their shared file list which were not downloaded by the client software but were instead acquired by other means.

21. The BitTorrent Network bases all of its file shares on the Secure Hash Algorithm (SHA1). This mathematical algorithm allows for the digital fingerprinting of data. Once you check a file or files with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that will be a fixed-length unique identifier for that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA1 is secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.

22. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

23. The computer running P2P software has an IP address assigned to it while it is connected to the Internet. Investigators are able to see the IP address of any computer system sharing files. Investigators can then search public records that are available on the Internet to

determine the specific Internet Service Provider (ISP) who has assigned that IP address to that computer. ISP's maintain logs and records which reflect the specific IP addresses it assigned to specific computers that connect to the Internet through that ISP at any given moment. Based upon the IP address assigned to the computer sharing files, subscriber information then can be obtained from the ISP which contains identifying information of the individual to whom the account is registered.

FACTS RELATING TO PROBABLE CAUSE

24. On July 20, 2021, your affiant was connected to the BitTorrent P2P network conducting investigations into the sharing of child pornography over the Internet. The investigation was focused to a device at IP address 137.103.160.62 because it was associated with a torrent with the infohash: 983904bc3b32f025f384048085c0de7618bcb8bf. This torrent file references a file identified as being a file of investigative interest to child pornography investigations. Using a law enforcement computer located at the Homeland Security Investigations office in Pittsburgh, Pennsylvania running investigative BitTorrent software, a connection was made to the device at IP address 137.103.160.62, hereinafter referred to as "Suspect Device". The Suspect Device reported it was using BitTorrent client software Transmission 2.94. On or about July 20, 2021, from 1651 hours and 1751 hours (UTC -4:00:00), your affiant downloaded approximately three files and partially downloaded approximately six files, that the Suspect Device was making available. The Suspect Device at IP Address 137.103.160.62 was the sole candidate for the download, and as such, the file was downloaded directly from this IP Address. Your affiant has reviewed the downloaded files and observed multiple videos that depict prepubescent minor females engaged in sexually explicit conduct. Your affiant describes one of these files as follows:

a. A video with file name 000005.avi that is approximately five minutes and 43 seconds in length depicts a prepubescent minor female with brown hair, estimated to be 8 to 10 years of age, performing oral sex on an adult male visible from stomach to feet. The video then shows a second prepubescent minor female estimated to be 6-8 years of age and a third minor female estimated to be 8 to 10 years of age, and both minor female's breasts and vagina are exposed to the camera. The video then shows the first minor female again lying on her back with breasts and vagina exposed as the camera zooms in and shows an adult male's hand touching her vagina.

25. On August 24, 2021, your affiant was connected to the BitTorrent P2P network conducting investigations into the sharing of child pornography over the Internet. The investigation was focused to a device at IP address 137.103.160.62 because it was associated with a torrent with the infohash: 610b27f1d2639e9d697aecc56d05a8510d6f7550. This torrent file references a file identified as being a file of investigative interest to child pornography investigations. Using a law enforcement computer located at the Homeland Security Investigations office in Pittsburgh, Pennsylvania running investigative BitTorrent software, a connection was made to the device at IP address 137.103.160.62, hereinafter referred to as "Suspect Device". The Suspect Device reported it was using BitTorrent client software -TR2940- Transmission 2.94. On or about August 24, 2021, from 0359 hours and 0553 hours (UTC -4:00:00), your affiant downloaded approximately 83 files that the Suspect Device was making available. The Suspect Device at IP Address 137.103.160.62 was the sole candidate for the download, and as such, the file was downloaded directly from this IP Address. Your affiant has reviewed the downloaded files and observed multiple videos that depict prepubescent minor females engaged in sexually explicit conduct. Your affiant describes one of these files as follows:

a. A video with file name 000284.avi that is approximately one minute and one second in length depicts multiple segments of a prepubescent minor female with brown hair wearing dark sunglasses, estimated to be 8 to 10 years of age. The first segment shows the minor female nude, standing in a shower with her arms behind her head, facing the camera with her breasts and vagina predominately displayed. The next segment shows

> same minor female lying on her back on a bed with white pillows and blue and white sheets, while a partially viewable adult male attempts to insert his penis into her vagina. The next segment shows the minor female seated on top of the nude adult male on a bed and having sexual intercourse. The next segment shows the minor female masturbating the adult male. The last segment shows the minor female fully dressed in a blue t-shirt, blue pants, and blue headband, standing next to the bed.

26. A check of publicly available records located online by an organization known as the American Registry of Internet Numbers, determined that the IP address 137.103.160.62 was assigned to a company known as Atlantic Broadband on July 20, 2021. On or about July 28, 2021, a federal summons to identify the IP Address history of the subscriber of IP address 137.103.160.62 was served to Atlantic Broadband. On or about July 28, 2021, a response to the summons identified that on July 20, 2021, from 1651 hours and 1751 hours (UTC -4:00:00), and August 24, 2021, from 0359 hours and 0553 hours (UTC -4:00:00), the subscriber was JOSEPH and LUCIEN SCOTT with the address **1008 21ST AVE., ALTOONA, PA 16601**.

27. On or about July 28, 2021, your affiant conducted a check in Pennsylvania Department of Transportation records which revealed identification number 34004779 had been issued to LUCIEN MALLORY SCOTT with the date of birth March 30, 2001. The address listed on this identification is **1008 21ST AVE., ALTOONA, PA 16601**.

28. On or about August 13, 2021, your affiant conducted a record check with the Pennsylvania Office of the Inspector General which revealed that in May of 2021, JOSEPH and LUCIEN SCOTT had reported the address **1008 21ST AVE., ALTOONA, PA 16601** in relation to an application for state benefits. The date of birth on this record for JOSEPH SCOTT is April 17, 1978. The date of birth on this record for LUCIEN SCOTT is March 30, 2001.

29. On or about August 30, 2021, your affiant conducted surveillance at **1008 21ST AVE., ALTOONA, PA 16601**. During this surveillance, your affiant observed and obtained

photographs of the residence. Your affiant can describe this residence as a three (3) story, single family residence, primarily of red brick construction with enclosed porch with white siding, gray roof, and entrance located at 21st Avenue. The numbers "1008" are displayed in black text on the white siding near the entrance door.

CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN CHILD PORNOGRAPHY AND WHO HAVE A SEXUAL INTEREST IN CHILDREN AND IMAGES OF CHILDREN

30. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and receive multiple visual depictions of minors engaged in sexually explicit conduct are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Such individuals almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica[1], and videotapes for many years.

b. Likewise, such individuals often maintain their collections that are in a

1 Child erotica, as used in this Affidavit and Attachments, is defined as items or depictions that may be sexually arousing to individuals with a sexual interest in children but which may not be obscene in and of themselves and do not necessarily depict minors engaged in sexually explicit conduct. Such materials may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.

digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

c. Such individuals also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/ collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

d. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

CONCLUSION

31. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B) may be located in the residence located at **1008 21ST AVE., ALTOONA, PA 16601** (more fully described in Attachment A).

32. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

33. It is further respectfully requested that this Court issue an Order sealing, until further order of Court, all papers submitted in support of this Application, including the Application, Affidavit, and the Search Warrant, and the requisite inventory notice (with the

exception of one (1) copy of the warrant and inventory notice that will be left at **1008 21ST AVE., ALTOONA, PA 16601**). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact of this continuing investigation and may jeopardize its effectiveness.

34. The above information is true and correct to the best of my knowledge, information and belief.

Respectfully submitted,

/s/ Jason Adams
JASON ADAMS
Special Agent
Homeland Security Investigations

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 13th day of October 2021.

HONORABLE KEITH A. PESTO
United States Magistrate Judge